

AMENDMENTS TO THE DRAWINGS

Replacement formal drawings of Figures 2 and 6 are attached hereto.

Attachments:

1. Replacement formal drawing of Figures 2 and 6
2. Annotated marked-up drawing of Figures 2 and 6

REMARKS

This communication is a full and timely response to the aforementioned non-final Office Action dated April 26, 2007. By this communication, claims 1 and 7-13 and 15-17 are amended, claim 14 is cancelled, and claims 20-27 are added. Claims 2-6, 18 and 19 remain in their original form. Thus, claims 1-13 and 15-27 are pending in the application. Reexamination and reconsideration of the application are requested in view of the foregoing amendments and the following remarks.

I. Replacement Formal Drawings

Replacement formal drawings of Figures 2 and 6 are submitted herewith to correct minor informalities in original Figures 2 and 6. In particular, original Figure 2 labels the operation panel 108 as an "OPERATIONAL PANEL". Accordingly, Figure 2 has been revised to label the operation panel 18 as an "OPERATION PANEL".

Figure 6 illustrates that a hash value is obtained from a self-made certificate. However, the second box from the top on the right hand side of original Figure 6 labels the obtained hash value as a "HUSH VALUE". Accordingly, Figure 6 has been revised to label this box as a "HASH VALUE".

Applicant submits that no new matter has been added via the editorial revisions to Figures 2 and 6. Accordingly, approval and entry of the replacement formal drawings of Figures 2 and 6 are respectfully requested.

For the Examiner's convenience, annotated marked-up drawings of Figures 2 and 6 are also submitted herewith to illustrate the revisions made to original Figures 2 and 6.

II. Amendments to the Specification

The specification has been carefully reviewed and revised in order to correct grammatical and idiomatic informalities to aid the Examiner in further consideration of the application. The above editorial amendments to the specification do not add new matter. Accordingly, approval and entry of the amendments to the specification are respectfully requested.

III. Objection to Information Disclosure Statement

The Examiner objected to the First Information Disclosure Statement (IDS) filed on September 29, 2003 for allegedly not complying with the requirements of 37 CFR 1.98(a)(1). Contrary to the Examiner's assertion, the Form PTO-1449 submitted with the First IDS complies with the five requirements (1)-(5) identified in the Office Action. Furthermore, it is noted that the Examiner returned an Examiner-initialed copy of the September 29, 2003 Form PTO-1449 to indicate that the references listed thereon were considered. Accordingly, Applicant respectfully requests that the objection to the First IDS be withdrawn.

IV. Request for Proper Citation of Applied Reference

The Examiner applied "Slick (US PGPub. No. 2004/01109568)" in rejecting claims 9, 11, 14, 15 and 19 on page 11 of the Office Action. Applicant notes, however, that the Slick et al. reference was not cited on the Form PTO-892 attached to the Office Action. As a result, the Slick reference is not properly of record in the present application. Accordingly, Applicant respectfully requests the Examiner to properly cite the Slick reference on a Form PTO-892 with the next action issued by the Office. Furthermore, the Examiner is respectfully requested to note the typographical error contained in the citation of the Slick reference on page 11 of the Office Action. The proper citation of the Slick reference is 2004/0109568 (2004/01[[1]]09568).

V. Correction of Claims

An exemplary embodiment of the present invention provides a communication system and method in which a device and a client securely communicate data with each other through a network, without requiring the device or client to obtain an electronic certificate from an authority outside the network to verify each other. For example, as shown in Figure 1, a device 100 communicates with a client 200 through a network 300. In the exemplary embodiment, the device 100 stores a root certificate 126 (see Figure 2), and the same root certificate 126 is stored in the client 200 as a root certificate 222 prior to a communication of the data between the device 100 and the client 200 (see Figure 3 and paragraph [0026]).

The root certificate 126, 222 includes a public key paired with a private key. Paragraph [0037] on pages 14 and 15 of the specification describes the operation of creating the root certificate 126, 222. In particular, the specification provides that the root certificate 126, 222 including the public key paired with the private key is signed (encrypted) with the private key (see step S16 in Figure 7, for example).

The above-described exemplary embodiment is encompassed in independent claims 1, 7 and 17. However, original claims 1, 7 and 17 contained a typographical error. In particular, original claims 1, 7 and 17 recited that the root certificate is signed with the public key. Accordingly, consistent with the above-described exemplary embodiment, claims 1, 7 and 17 have each been amended to recite that the root certificate, which includes the public key paired with the private key, is signed with the private key.

VI. Rejections Under 35 U.S.C. §112

Claim 7 was rejected under 35 U.S.C. §112, second paragraph, for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Claim 7 has been amended to recite that the client installs the root certificate which is held in the device.

Applicant submits that claim 7 particularly points out and distinctly claims the subject matter which the Applicant regards as the invention. Accordingly, Applicant respectfully requests that the indefiniteness rejection of claim 7 be withdrawn.

VII. Rejections Under 35 U.S.C. §102

Claims 13 and 16 were rejected under 35 U.S.C. §102(e) as being anticipated by Smetters et al. (U.S. Patent Publication No. 2004/0088548, hereinafter "Smetters").

Claim 13 has been amended to include the limitations recited in cancelled claim 14. The rejection of claim 14 is respectfully traversed below.

VIII. Rejections Under 35 U.S.C. § 103

A. Claims 1, 4-5, 7-8, 10, and 12 were rejected under 35 U.S.C. §103(a) as being unpatentable over Smetters in view of Aiello et al. (U.S. Patent No. 6,397,329, hereinafter "Aiello"), and further in view of Benson (U.S. Patent No. 6,047,242). Applicant respectfully traverses this rejection.

Claim 1 recites a communication system in which a device and a client communicate data with each other through a network. The device is recited in claim 1 as comprising a first storage device which stores a root certificate including a public key paired with a private key and being signed with the private key. Claim 1 recites that the device also comprises a certificate creator which creates a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key. The device is also recited in claim 1 as comprising a communication device which transmits the second certificate created by the certificate creator to the client.

Claim 1 recites that the client comprises a second storage device which stores the root certificate stored in the first storage device. Further, the client is recited in claim 1 as comprising a verifier which verifies the signature of the second certificate received from the device with the root certificate stored in the second storage device.

Claim 7 recites a method in which the device and client perform steps corresponding to the constituent elements of the communication system of claim 1.

Smetters discloses a system for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2) (see Figures 1 and 3). The first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and encryption when providing the device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) generates a root certificate 30 for the space 20 and digitally signs the root certificate 30 (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4). Then, the first device 12(1) sends an invitation message to the second device 12(2) and establishes a secure communication channel with the second device 12(2) by sending a range-limited signal including a

public key used to secure the communication between the devices 12(1), 12(2) (see paragraphs [0028]-[0030], and steps 200 and 300 in Figure 2). Smetters discloses that the second device 12(2) then decides whether to use a particular public key (e.g., the public key included in the range-limited signal from the first device 12(1)) or a public key generated by the first device 12(1) to communicate with the first device 12(1) (see paragraph [0032] and step 510 in Figure 6). If the second device 12(2) decides to use a particular public key, the second device 12(2) transmits this public key to the first device 12(1) (see paragraph [0032] and step 520 in Figure 6). On the other hand, if the second device 12(2) decides to use a public key generated by the first device 12(1), the first device 12(1) generates a pair of a public key and a private key, and sends the private key of the generated key pair to the second device 12(2) (see paragraph [0033], and steps 530 and 540 in Figure 6).

To provide the second device 12(2) with access to the shared space 20, Smetters discloses that the first device 12(1) then creates a second certificate 40 using either the public key sent from the second device 12(2) or the public key of the key pair generated by the first device 12(1). The second certificate 40 designates the second device 12(2) as a member of the shared space 20 and is equivalent to the root certificate 30 (see paragraphs [0031] and [0034], step 500 in Figure 2, and step 550 in Figure 6). Then, the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2), and the second device 12(2) stores the received root certificate 30 and second certificate 40 in a memory thereof (see paragraph [0035] and step 600 in Figure 2). The root certificate 30 and the second certificate 40 stored in the second device 12(2) form a "certificate chain", which the second device 12(2) uses to prove to other devices 12(3) that the second device 12(2) is an authorized member of the shared space 20 (see paragraph [0035]). The "certificate chain" of the first device 12(1) is only the root certificate 30. If the second device 12(2) desires the first device 12(1) to verify that it is a legitimate provider of access to the space 20, the first device 12(1) presents its certificate chain (i.e., the root certificate 30) and proof of possession of the private key corresponding to the public key used to create the second certificate 40 to the second device 12(2) (see paragraph [0042]).

As acknowledged by the Examiner, Smetters does not disclose or suggest that the root certificate 30 is signed with a public key. The Examiner applied Aiello to teach this feature, because Aiello discloses that a certificate may be signed by a public key of a third party certificate authority (CA) (see Column 4, lines 54-55).

However, as described above, claims 1, 7 and 17 have each been amended to recite that the root certificate is signed with the private key paired with the public key in the root certificate. Accordingly, the application of Aiello for signing a root certificate with a public key is no longer believed to be relevant to the claimed invention.

As acknowledged by the Examiner, neither Smetters nor Aiello disclose a second certificate being signed with a private key, as recited in claims 1 and 7. In an attempt to teach this feature, the Examiner applied Benson.

Benson discloses a software protection system in which a challenge means accesses a trusted root certificate. Benson discloses that a root certificate is used to authenticate a descendent certificate, which holds a public key of a trusted source. The descendent certificate is reached from the root certificate via a certificate path, similar to the "certificate chain" disclosed in Smetters (see Column 2, lines 62-65 and Column 9, lines 46-55).

The Examiner relied on Benson in an attempt to cure the deficiencies of Smetters and Aiello for failing to disclose or suggest a second certificate being signed with a private key. However, Benson discloses that "root certificates are signed using the certificate authority's private key" (see Column 2, lines 62-63) (emphasis added). Benson, however, does not disclose or suggest that the descendent certificates are signed with a private key of the certificate authority (CA), particularly a private key included in the root certificate, as recited in claims 1 and 7.

Claims 1 and 7 recite that the second certificate designates the root certificate as a certificate authority at a higher level. Accordingly, the second certificate recited in claims 1 and 7 corresponds to the "descendent certificate" of Benson. As described above, Benson does not disclose or suggest that the descendent certificate is signed with a private key of the CA or a private key included in the root certificate. Instead, Benson merely discloses that the descendent certificate is

reached (or validated) from the root certificate via a certification path, and that the descendent certificate holds a public key of a trusted source.

Accordingly, contrary to the Examiner's assertion, Benson does not disclose or suggest a second certificate (descendent certificate) being signed by the private key included in the root certificate, as recited in claims 1 and 7.

Therefore, the combination of Smetters, Aiello and Benson, either individually or in combination, fails to disclose or suggest each and every limitation of claims 1 and 7.

Consequently, no obvious combination of Smetters, Aiello and Benson would result in the inventions of claims 1 and 7, since Smetters, Aiello and Benson, either individually or in combination, fail to disclose or suggest each and every limitation of claims 1 and 7.

Therefore, for at least the foregoing reasons, Applicant submits that claims 1 and 7 are clearly patentable over Smetters, Aiello and Benson.

In addition to the patentability of independent claims 1 and 7, Applicant submits that dependent claims 8 and 20-24 of claims 1 and 7 recite further distinguishing features over Smetters, Aiello and Benson.

New claim 20 recites that the root certificate stored in the first storage device is stored in the second storage device prior to the transmission of the second certificate from the communication device. New claim 21 recites that the root certificate stored in the first storage device is stored in the second storage device prior to initiation of communication between the device and the client. New claim 23 recites that, in the method of claim 7, the device sends the second certificate to the client after the root certificate is installed in the client.

As described above, Smetters discloses that after the second device 12(2) has accepted the invitation from the first device 12(1), the first device 12(1) creates the second certificate 40 and then sends "both the root certificate 30 and the second laptop member certificate 40 to the [second device] 12(2)" (see paragraph [0035]) (emphasis added). Accordingly, since the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device at the same time after the second certificate 40 is created, Smetters clearly does not disclose or suggest the above-described limitations of new dependent claims 20, 21 and 23.

Aiello and Benson also clearly fail to disclose or suggest the limitations of new claims 20, 21 and 23.

New claim 22 recites that the verifier of the client is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in the second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from the device, and comparing the first and second hash values to determine if they are equal to each other. Smetters, Aiello and Benson each fail to disclose or suggest this verification procedure recited in new claim 22.

Claim 8 recites that the device further holds at least one intermediate certificate for one or more certificate authorities existing in a hierarchical order up to a root certificate authority. In addition, claim 8 recites that the client installs the at least one intermediate certificate in addition to the root certificate, and the device sends the second certificate to the client. Further, claim 8 recites that the client verifies the signature of the second certificate received from the device with the at least one intermediate certificate installed therein, and verifies the signature of the at least one intermediate certificate received from the device with the root certificate installed therein.

Claim 8 was rejected as being unpatentable over the combination of Smetters, Aiello and Benson. In particular, the Examiner alleged that the limitations recited in claim 8 are disclosed by Smetters. Applicant respectfully submits that the Examiner has inconsistently interpreted the disclosure of Smetters in rejecting claim 8.

Smetters discloses that once the second device 12(2) has received both the root certificate 30 and the second certificate 40, the second device 12(2) may then give access to the shared space 20 to a third device 12(3). In effect, the second device 12(2) grants the third device 12(3) the access to the shared space 20 that it was granted by the first device 12(1) (see paragraph [0044]). After sending an invitation message and establishing a secure communication channel with the third device 12(3), the second device 12(3) creates a third certificate 50 for the third device 12(3), and sends the "certificate chain" to the third device 12(3). Here, the "certificate chain" includes the root certificate 30 created by the first device 12(1), the

second certificate 40 created by the first device 12(1) for the second device 12(2), and the third certificate 50 created by the second device 12(2) for the third device 12(3) (see paragraph [0045] and Figure 7).

By depending from claim 7, claim 8 further defines the limitations recited in claim 7. Claim 7 recites that the device creates and sends the second certificate to the client. Therefore, the "device" of claims 7 and 8 corresponds to the first device 12(1) of Smetters, and the "client" of claims 7 and 8 corresponds to the second device 12(2) of Smetters.

The second device 12(2) of Smetters cannot correspond to the "device" of claims 7 and 8 because the second device 12(2) does not create the second certificate 40, in contrast to claim 7. The second device 12(2) creates the third certificate 50, which is the lowest certificate in the hierarchy of the "certificate chain" received by the third device 12(3). On the other hand, the second certificate recited in claim 8 is the lowest certificate in the hierarchy of a certificate chain, because the client is recited in claim 8 as verifying the signature of the second certificate with the at least one intermediate certificate installed in the client, and verifying the signature of the at least one intermediate certificate with the root certificate installed in the client. Thus, the at least one intermediate certificate of claim 8 corresponds to the second certificate 40 of Smetters, and the second certificate of claim 8 corresponds to the third certificate 50 of Smetters.

However, in contrast to claim 8, the first device 12(1) of Smetters, which corresponds to the device of claim 8, does not send the third certificate 50 to the second device 12(2). Instead, as described above, the second device 12(2), independent of the first device 12(1), creates and sends the third certificate 50 (corresponding to the second certificate of claim 8) to the third device 12(3). Accordingly, Smetters does not disclose or suggest the step of the device sending the second certificate to the client, as recited in claim 8.

Furthermore, Smetters discloses that the third device 12(3) verifies the third certificate 50 by using the second certificate 40. Accordingly, Smetters also does not disclose or suggest that the client (second device 12(2)) verifies the signature of the second certificate (third certificate 50) received from the device (first device 12(1)) with the at least one intermediate certificate (second certificate 40) installed therein,

and verifies the signature of the at least one intermediate certificate (second certificate 40) received from the device (first device 12(1)) with the root certificate (root certificate 30) installed therein, as recited in claim 8.

New claim 24, which depends from claim 8, recites that the client installs the at least one intermediate certificate prior to receiving the second certificate from the device. Smetters clearly does not disclose or suggest this limitation for two reasons. First, the second device 12(2) (client of claim 8) does not receive the third certificate 50 (corresponding to the second certificate of claim 8). Second, even if the second device 12(2) did receive the third certificate 50, the third certificate 50 is sent at the same time with the first and second certificates 30, 40 as a "certificate chain".

Accordingly, Applicant submits that Smetters clearly does not disclose or suggest the limitations of claims 8 and 24. Aiello and Benson also clearly fail to disclose or suggest the limitations of claims 8 and 24.

For at least the foregoing reasons, Applicant submits that Smetters, Aiello and Benson, either individually or in combination, clearly do not disclose or suggest the limitations of claims 8 and 20-24.

Therefore, in addition to the patentability of claims 1 and 7 demonstrated above, Applicant respectfully submits that claims 8 and 20-24 are clearly patentable over Smetters, Aiello and Benson.

B. Independent claim 17 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Aiello.

Claim 17 has been amended to recite that the device comprises a certificate creator which creates a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key. As acknowledged by the Examiner, Smetters and Aiello fail to disclose or suggest this feature of the invention. The Examiner applied Benson in an attempt to teach this feature. However, as demonstrated above, Benson discloses that a root certificate, not a descendent certificate (second certificate), is signed with a private key. Accordingly, Smetters, Aiello and Benson clearly do not disclose or suggest each and every limitation of claim 17.

New claim 25 recites a device to be used in a communication system in which a device and a client communicate with each other through a network. Similar to claim 17, the device of new claim 25 comprises a second storage device which stores a root certificate signed with the public key. The device of new claim 25 also comprises a certificate creator which creates a second certificate designating the root certificate as a certificate authority at a higher level. In addition, the device of new claim 25 comprises an interface which sends the information as well as the root certificate including the public key to the client through the network, and sends, after the root certificate is installed in the client, the second certificate to the client for verification of the information sent from the device.

As described above, Smetters discloses that after the first device 12(1) creates the second certificate 40 for the second device 12(2), the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2) as a "certificate chain" (see paragraph [0035]). Accordingly, in contrast to new claim 25, Smetters does not disclose or suggest a device comprising an interface which sends, after the root certificate is installed in the client, the second certificate to the client for verification of the information sent from the device. Aiello and Benson also fail to disclose or suggest this limitation of new claim 25.

Accordingly, for at least the foregoing reasons, Applicant submits that claims 17 and 25 are also clearly patentable over Smetters, Aiello and Benson, since Smetters, Aiello and Benson, either individually or in combination, do not disclose or suggest each and every limitation of claims 17 and 25.

C. Claims 9, 11, 14, 15 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Aiello, Benson and Debry (U.S. Patent No. 6,918,042) and further in view of Slick (U.S. Patent Application Publication No. 2004/01109568).

As described above, independent claim 13 has been amended to include the limitations recited in cancelled claim 14. Accordingly, claim 13 recites a computer-readable storage device storing a program which causes a computer to execute operations of requesting a root certificate from a device connected to the computer through a network, and receiving the root certificate from the device. In addition,

claim 13 recites that the program causes the computer to execute operations of converting the received root certificate to a predetermined format upon receiving the root certificate, and installing the converted root certificate.

The Examiner alleged that the operations of converting the received root certificate to a predetermined format and installing the converted root certificate are obvious in view of the disclosure of Smetters. In particular, with reference to paragraph [0026] of Smetters, the Examiner opined "it is well known in the art for any of these certificates to be converted to one standard in order to communicate with each other". Paragraph [0026] of Smetters does not, in any reasonable way, support this conclusory assertion.

In particular, paragraph [0026] of Smetters discloses that while the system 10 utilizes standard cryptographic authentication techniques and creates a public key infrastructure ("PKI") to allow members of a shared space 20 to prove their membership to each other, other authentication and cryptographic techniques may be used, such as group signature schemes, identify-based-encryption, storage of lists of public keys or pre-existing certificates, shared secrets or anonymous credentials. In addition, paragraph [0026] discloses that while X.509 public key certificates are used in the described embodiment, other certificate types, such as XML certificates, SPKI certificates, WTLS certificates or attribute certificates may be used.

This disclosure of Smetters merely provides alternative cryptographic techniques that may be used instead of the techniques used in the described embodiments. Contrary to the Examiner's conclusory assertion, this disclosure of Smetters does not disclose or suggest that it is well known in the art to convert certificates formed in one technique to a certificate in another technique. Furthermore, Aiello provides an extensive discussion of cryptography techniques used in the art, but at no point does Aiello even remotely suggest that the techniques are mutually convertible.

In using the claims as a template to combine bits and pieces of various references to attempt to result in the claimed invention, the Examiner applied a multifaceted combination of six different references. None of the six applied references provide support for the Examiner's opinion that it is well known in the art

to convert one type of cryptographic certificate to another type of cryptographic certificate. In the absence of documentary evidence to the contrary, Applicant submits that the ostensibly well-known feature of converting a certificate to a certificate of a different technique is not disclosed or suggested by any of the references of record.

Accordingly, Applicant respectfully submits that claim 13 is patentable over the applied references since none of the applied references disclose or suggest the converting operation recited in claim 13.

Dependent claim 9 also recites this feature of the present invention. Applicant submits that claim 9 is also patentable over the applied references for the same reasons as claim 13.

D. Dependent claims 2 and 3 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Aiello and Benson and further in view of Debry. Dependent claim 6 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Aiello and Benson and further in view of Vogel et al. (U.S. Patent No. 6,816,900, hereinafter "Vogel"). Dependent claim 18 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Aiello and further in view of Debry.

As demonstrated above, Smetters, Aiello and Benson fail to disclose or suggest each and every limitation of independent claims 1, 7, 13, 17 and 25 as well as dependent claims 8, 9 and 20-24. Slick, Derby and Vogel, either individually or in combination, do not cure the deficiencies of Smetters, Aiello and Benson for failing to disclose or suggest each and every limitation of claims 1, 7, 13, 17 and 25 as well as dependent claims 8, 9 and 20-24.

Therefore, no obvious combination of Smetters, Aiello, Benson, Slick, Derby and Vogel would result in the inventions of claims 1, 7-9, 13, 17 and 20-25, since these references, either individually or in combination, fail to disclose or suggest each and every limitation of claims 1, 7-9, 13, 17 and 20-25.

Furthermore, in view of the clear distinctions discussed above, one skilled in the art would not have been motivated to modify Smetters, Aiello, Benson, Slick,

Derby and Vogel in such a manner as to result in, or otherwise render obvious, the inventions of claims 1, 7-9, 13, 17 and 20-25.

Consequently, Applicant respectfully submits that claims 1, 7, 13, 17 and 25, as well as claims 2-6, 8-12, 15, 16, 18-24, 26 and 27 which depend therefrom, are clearly patentable over the references applied by the Examiner.

IX. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

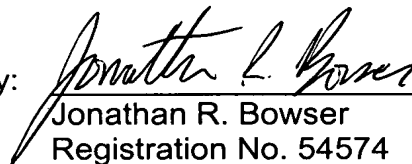
A fee and a Petition for a two-month Extension of Time are filed herewith pursuant to 37 CFR § 1.136(a).

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 19, 2007

By:


Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620



Fig. 2

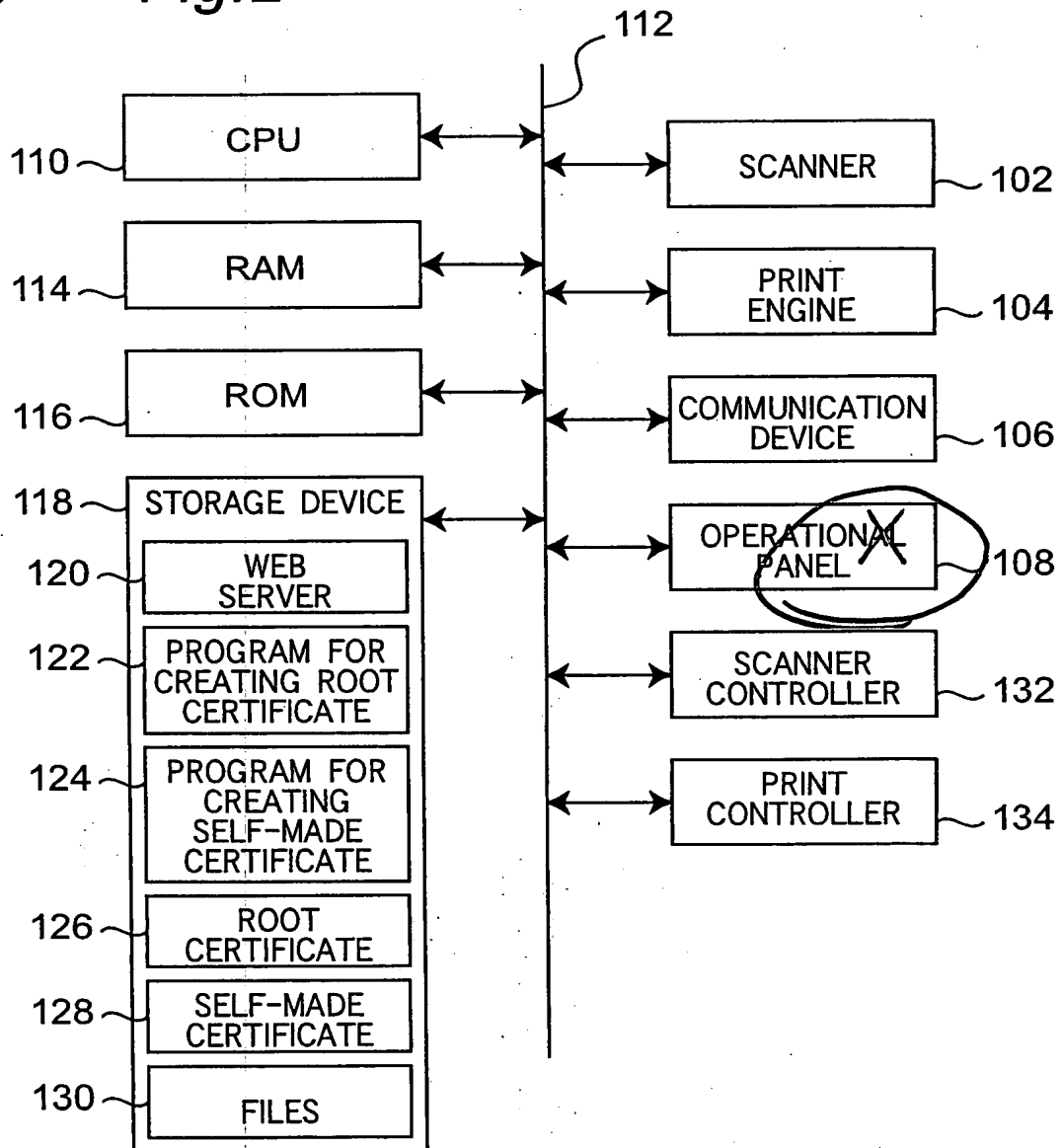




Fig. 6

